Data Protection as a Pillar of Humanitarian Accountability: Workshop part of the series of events related to the CoD Resolution on *Principled and Accountable Use of Information and Communication Technologies in Humanitarian Action*

Introduction

On May 18, 2026, the IFRC and ICRC Data Protection Offices, supported by National Societies and Civil Society Organizations, held an online workshop on using data protection to enhance accountability in humanitarian action.

This initiative, part of the work that the Working Group for the Resolution on *Principled and Accountable Use of Information and Communication Technologies in Humanitarian Action* is doing to spread awareness on the goals of the Resolution and collect input from members of the Movement, aimed to:

- Promote a protection-oriented approach to ICT use, safeguarding the rights and dignity of affected populations.
- Emphasize data protection as a key tool for accountability and a way to operationalize humanitarian principles in digital contexts.
- Encourage National Societies to reflect on their data protection practices and their impact on technology use.
- Highlight the Movement's progress in data protection while addressing remaining gaps and fostering collaboration.

The workshop included two segments: (I) sharing practical examples from National Societies and Civil Society Organizations on data protection and accountability, and (II) group discussions in breakout rooms on gaps, lessons, and opportunities for integrating data protection as driver for accountability into the draft Resolution.

I. Data Protection as a Tool for Accountability

Accountability vis-à-vis affected individuals and authorities
Charo Solanes ***Head of Data Protection Office*** ***Spanish Red Cross*** <u>Key Takeaways</u> • **Data protection is enforceable accountability**. It is not just formal compliance. Data Protection regulation in many countries establishes concrete rights for individuals and sanctionable obligations for organisations. When we fail to ensure data protection, we answer to an independent authority and to the people affected.

- **The DPIA is the first level of preventive accountability**. Conducting one properly forces the identification of risks before they materialise.
- **Having protocols is not enough**. they must be applied and verified. The gap between internal standards and actual practice is the greatest point of vulnerability
- **The DPO is the strategic interlocutor with the supervisory authority.** An active DPO makes a difference: they notify the breach on time, manage the investigation, submit substantiated arguments, and can reduce the severity and amount of sanctions.
- **Consequences are both economic and reputational**. In humanitarian organisations, trust is a critical asset: without it, we cannot reach people or secure resources.
- **The same standards must apply in international humanitarian contexts.** If populations affected by conflict or disaster trust their data to our organisations, they deserve the same level of protection.
- **Data protection is not a burden: it is a guarantee of dignity.** People retain the right to control their most intimate information even when they entrust it to those who want to help them. Protecting that data is, in itself, a humanitarian act.

Additional Resources
https://www.aepd.es/documento/ps-00487-2024.pdf

Contact
rsc@cruzroja.es

Accountability through civil society

Alexandrine Pirlot de Corbion
Director of Strategy
Privacy International

Key Takeaways

- **Defining the Digital Ecosystem**. The digital ecosystem encompasses people, data, services, and broader infrastructure. There is an increasing overlap between data and technology across the humanitarian sector, conflict zones, and civilian contexts. This overlap has significant implications for individuals and organizations, particularly regarding accountability.
- **Data Protection as Accountability**. Data protection should be framed as a practical accountability mechanism. It defines and shapes the responsibilities of both public and private sector actors.
- **Examples Across Contexts**:
  - **Humanitarian/Aid Settings**: Use of technologies like ID systems and biometrics.
  - **Conflict and Militarization of Technology**: Risks such as data centers being targeted as military assets.
  - **Civilian Contexts**: Issues like the use of surveillance tools and their implications for privacy and accountability.

Additional Resources

Contact
alex@privacyinternational.org

Victor Ndede
Head of Programmes
Amnesty International Kenya

Key Takeaways

- **Shift Focus to Affected People**. Data protection should prioritize the perspectives and needs of beneficiaries rather than just institutional policies.
- **True Transparency Beyond Consent**. Move away from complex, jargon-filled consent forms. Ensure communication is accessible, multilingual, and culturally relevant so beneficiaries clearly understand how their data will be used, who will access it, and for how long.
- **Establish Recourse Mechanisms**. Accountability requires clear, safe, and accessible channels for beneficiaries to report data misuse or challenge automated decisions. These mechanisms must ensure no retaliation or loss of aid for those who raise concerns.
- **Risk Assessment from a Community Perspective**. Evaluate data risks by considering the potential harm to marginalized communities, such as physical violence, discrimination, or persecution, rather than focusing solely on corporate liability.
- **Embed Accountability in Risk Assessment**. Responsible technology use involves integrating accountability measures into every stage of assessing and managing data risks.

Additional Resources
https://www.amnestykenya.org/wp-content/uploads/2025/10/DPA-Awareness-Perception-Study-Final.pdf
https://www.amnestykenya.org/wp-content/uploads/2024/09/Maisha-Namba-Report-FINAL-EDIT.pdf

Contact
victor.ndede@amnesty.or.ke

Belkis Wille
Associate Director, Crisis, Conflict and Arms Division
Human Rights Watch

Key Takeaways

- **How data is used and secured can cause harm.** Information collected for humanitarian purposes can later be misused for surveillance, targeting, persecution, or forced return.
- **Consent has inherent limitations in humanitarian contexts.** When people cannot refuse data collection without losing access to aid, their agreement cannot be considered fully free or informed. Organisations must acknowledge this power imbalance and design their practices accordingly.
- **Biometric data collection carries disproportionate risks and is often unnecessary.** Effective aid delivery can be achieved without gathering sensitive biometric information, and organisations should carefully justify any exception to this principle.
- **Data minimisation is a frontline protection measure.** Collecting only what is strictly necessary for life-saving purposes directly reduces the potential for harm if data is compromised or misused.
- **Purpose creep poses a serious and underestimated risk.** When data is shared or repurposed beyond its original scope, people can be exposed to consequences they never anticipated or

consented to.

- **Voluntary data-sharing with State authorities is as significant a risk as breaches or leaks.** The dangers to affected populations do not stem only from external attacks. Deliberate disclosure to governments can be equally harmful.
- **Refugees and displaced people are disproportionately exposed.** They face the highest data-related risks while benefiting from the fewest legal protections, making heightened caution and care essential in operations involving these groups.
- **Identity systems are not neutral tools.** Depending on how they are designed and governed, they can either support access to rights and services or become instruments of exclusion and control.
- **Data protection as a way to ensure "Do no harm".** Data protection is not an IT or compliance function; it is a core responsibility of humanitarian protection work at every level of an organisation.

Additional Resources
https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans
https://www.hrw.org/news/2023/07/11/you-dont-need-demand-sensitive-biometric-data-give-aid-ukraine-response-shows-how
https://www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected
https://hakinasheria.org/impact/legal-identity-citizenship/

Contact
willeb@hrw.org

Training and Capacity Building

Jonathan Lopez Marquez
National Coordinator for Migration and RFL
Argentine Red Cross

Key Takeaways

- **Data protection is not a bureaucratic burden but a humanitarian imperative.** In sensitive programmes such as Restoring Family Links (RFL) or Human Mobility, data protection is directly linked to the preservation of human dignity.
- **"Do No Harm" applies to data.** Proactively mitigating any negative impact means ensuring that the capture, storage, and transmission of personal data are carried out in a strictly ethical and secure manner.
- **Decentralised, self-assisted training is key to scalability.** One of the main challenges is standardising technical knowledge across all territorial branches, replicating training sessions locally without dedicated budgets or extensive time. The solution developed by the ARC lies in adapting formal procedures into user-friendly virtual learning platforms, with methodological support from the ICRC.
- **Training teams to deliver transparent information transforms power dynamics.** When field staff are equipped to explain the use of data in clear and simple terms and to genuinely welcome people's questions and reactions, they are exercising direct and measurable accountability and individuals cease to be treated as passive beneficiaries and are recognized as rights holders and owners of their own data, restoring control and dignity.

- **Poor data management can directly harm beneficiaries.** In contexts of migration and family separation, information managed carelessly can be misused against the very people we seek to help. Strengthening IT security and strictly limiting access is therefore a core protection responsibility.
- **Community trust is a precondition for effective humanitarian action.** If communities perceive negligence in the handling of their confidential information, the quality of data shared will deteriorate or people will stop seeking assistance altogether. Robust data protection sustains trust, community engagement, and the quality of the humanitarian response.

Additional Resources

- Virtual training course on RCF (can be consulted upon request)

Contact
jlmarquez@cruzroja.org.ar

Sharing Good Practices across Organizations

Mohamed Bahero
Innovation Officer, International Centre for Humanitarian Affairs (ICHA)
Kenya Red Cross

Key Takeaways

- **Sarafu Network Case Study**. The case study focuses on the measures implemented by the Kenya Red Cross Society (KRCS) to enhance data protection within the Sarafu Network.
- **Formal Partnership Agreement**. KRCS established a formal partnership with Grassroots Economics (the tech provider). The agreement includes specific data protection provisions to ensure accountability and compliance.
- **Volunteer Code of Conduct**. Project volunteers are required to sign a code of conduct that explicitly outlines their data protection responsibilities.
- **Data Minimization Principle.** The project applies data minimization principle, collecting only the data that is strictly necessary for the Sarafu Network to function effectively.

Additional Resources
https://red-social-innovation.com/en/solution/sarafus-the-community-currency-at-the-service-of-the-local-economy-in-kenya/
https://cash-hub.org/wp-content/uploads/sites/3/2020/10/CIC-Overview-short-latest-v5250919-public-viewing.pdf

Contact
bahero.mohamed@icha.net

Jason Sassine
Cybersecurity Manager
Lebanese Red Cross

Key Takeaways

- **AI Tool Design**. The Lebanese Red Cross (LRC) developed an AI tool with a strong focus on privacy and confidentiality throughout the design process.

- **Privacy and Confidentiality Considerations**. Specific measures were taken to ensure that sensitive data was protected and handled responsibly during the tool's development and implementation.
- **Demo as a Key Component**. A demo of the AI tool was conducted to test its functionality and ensure that privacy and confidentiality measures were effectively integrated.
- **Enhanced Accountability Frameworks**. By prioritizing privacy and confidentiality, the LRC was able to establish stronger accountability frameworks, ensuring trust and ethical use of the AI tool.

Additional Resources

Contact
jason.sassine@redcross.org.lb

II. Outcomes from the discussion in working groups

*The following summarises the key insights and recommendations that emerged from the five working group discussions held during the workshop. These outcomes reflect the collective experience of participants and are intended to inform the development of the **CoD Resolution on Principled and Accountable Use of Information and Communication Technologies in Humanitarian Action**.*

1. Data protection as a widely accepted legal framework to ensure accountability in the processing of personal data

Facilitators: **Emily Knox**, Head of Restoring Family Links, and **Milgo Ali**, Head of Information Governance and DPO, British Red Cross

Key Takeaways

- **Increased Establishment of Data Protection Frameworks at Global Level**: Awareness of data protection as a legal framework has grown significantly across many national contexts, and a growing number of supervisory authorities are moving from standard-setting to active enforcement.
- **Implementation Gap**: Implementation in daily operations remains the critical gap. Guidance for volunteers and frontline staff, as well as practical training, are often absent even where legal frameworks exist.
- **Emphasis on Data Protection Risk Assessments**: should be explicitly emphasised in the Resolution as a key step not only for selecting new technologies, but for ICT systems and programmes already in use.

The Resolution presents a vital opportunity to bridge the gap between growing legal awareness and practical implementation of data protection measures when adopting technological solutions to deliver humanitarian services. By emphasizing the importance of prior risk assessments and raising awareness on the need for the Movement to navigate and apply the national legal frameworks, the Resolution can help ensure that data protection becomes an integral part of daily operations across all contexts.

2. Risk assessments, design choices, and third-party dependencies

Facilitator**: Melanie Rideout**, AI Strategist, Swedish Red Cross

Key Takeaways

- **Risk Assessments as a Starting Point**: Risk assessments must be the foundation for deciding whether to adopt specific technology, rather than a box-ticking exercise conducted after decisions are made.
- **Risk Assessments as Living Documents**: Data protection risk assessments should be living documents, regularly revisited and updated to reflect project evolution, changes in technology, and shifts in data usage.
- **Lifecycle Perspective**: A lifecycle perspective on risk is essential, considering not only the risks of data processing within a project but also those related to third-party infrastructure (e.g., Azure, SharePoint, AWS, Google). This includes implementing robust security measures, such as local encryption, data shielding, or sovereign cloud solutions.
- **Budgetary Constraints**: Resource allocation for data protection infrastructure must be factored into operational planning from the outset, as budgetary constraints directly impact the quality of ICT governance and data protection measures.
- **Coordination Across Roles**: Embedding data protection into the design and use of ICTs requires active collaboration between data protection focal points and technical teams, ensuring risk assessments are conducted and reviewed throughout the project lifecycle.
- **Data Backup and Infrastructure Risks**: Risk assessments must extend beyond data collection and use to include the infrastructure on which data is stored and backed up. This is specifically relevant in programs where personal data of affected people are involved.

A proactive, lifecycle-based approach to risk assessment, supported by resources and cross-functional collaboration, is essential to embedding data protection into technology decisions. The Resolution offers a key opportunity to raise awareness across the Movement about the importance of this risk-based approach and to foster a coordinated effort to address shared challenges and improve data protection practices.

3. Data breaches and incident response as accountability in practice

Facilitator: **Quito Tsui**, Researcher and Writer, Humanitarian AI / MERL Tech Initiative

Key Takeaways

- **Proactive and Collaborative Approach:** Effective data breach response and protection require a proactive, collaborative, and well-resourced strategy.
- **Clear Roles and Responsibilities:** Organisations must define roles and responsibilities before incidents occur to ensure accountability and enable swift action.
- **Internal and External Risks:** While external cyberattacks often dominate attention, internal breaches, caused by human error, access mismanagement, or organisational failures, are equally critical and must not be overlooked.
- **Investment in Security Infrastructure:** Adequate budgeting for security measures is essential, not optional, to safeguard data and maintain accountability.

- **Collaboration and Shared Knowledge:** No single organisation has all the expertise or resources to address today's complex risk landscape. Collaboration, shared lessons, and pooled resources are vital.
- **Holistic Incident Response:** Incident response should be pre-emptive and embedded into organisational culture, going beyond legal or technical compliance to ensure comprehensive data protection.

Data breaches are becoming increasingly common, occurring in both digital and physical spheres. It is essential to identify key challenges and draw lessons from past incidents to ensure robust preparedness and effective response. A coordinated approach across the Movement, supported by the Resolution, could play a pivotal role in addressing these challenges, particularly in sharing expertise and experiences in handling data breaches, managing risks associated with the use of technological solutions to process the personal data of affected people, staff, and volunteers.

4. Data protection literacy and organizational capacity

Facilitator: **Katherine Wright**, Lead Restoring Family Links, Australian Red Cross

Key Takeaways

- **Existing Training Gaps**: While some data protection training exists across National Societies, its scope and depth remain insufficient. There is a clear need for more specialised capacity-building, including targeted training for not only staff but also volunteers to raise awareness across all levels of the Movement.
- **Awareness of National Legislations**: Awareness of national data protection laws is uneven across National Societies. It is critical for organisations to understand the legal frameworks governing their operations, including laws currently being discussed or in the process of adoption.
- **Integration into Operations**: Data protection should be embedded in operational decision-making rather than treated as a standalone compliance requirement. When integrated effectively, data protection strengthens humanitarian operations rather than constraining them.
- **From Theory to Practice**: The gap between theoretical understanding and practical application of data protection remains a challenge. While programmes like Restoring Family Links (RFL) demonstrate good awareness of data protection and associated risks, this level of understanding is not yet consistent across all programmes.
- **Promoting Accountability in Technology Use**: The Resolution should emphasise the importance of data protection in ensuring the accountable use of technologies within the Movement. This includes fostering awareness of data protection risks and responsibilities at all levels.

The Resolution offers a key opportunity to address gaps in data protection literacy and capacity across the Movement. By promoting awareness, supporting capacity-building, knowledge-sharing, and embedding data protection into operations when using a specific technological solution, it can help ensure more accountable and effective humanitarian responses in a data-driven world.

5. Strengthening accountability

Facilitator: **James de France**, Head of the IFRC Data Protection Office

Key Takeaways

- **Local-Level Training and Awareness:** The Resolution must ensure that sufficient training and awareness reach the local level, where data is collected and where the most significant accountability gaps tend to occur.
- **Resource Limitations**: Many National Societies lack dedicated staff to monitor data protection implementation and build knowledge among personnel, including volunteers.
- **Community-Centered Approach**: Communities and affected populations should be at the heart of the Movement's approach. People must be aware of their rights, and all Movement components and partners must be held accountable to them.
- **Bridging Knowledge Gaps and Building a Network:** Bridging knowledge gaps across the Movement requires deliberate mechanisms for sharing expertise, good practices, and operational lessons, both within and between organisations. This can be done through the increase of awareness within the Movement and the building of a network of data protection focal points and IT experts who can exchange on this topic at different levels (local, regional and global).

The Resolution can play a pivotal role in addressing accountability gaps by ensuring sufficient training and awareness reach the local level, where data is collected. It should promote resource allocation for dedicated data protection roles, empower communities by raising awareness of their rights, and establish mechanisms for sharing expertise and good practices across the Movement. By fostering a network of data protection focal points and IT experts at local, regional, and global levels, the Resolution can help bridge knowledge gaps and strengthen accountability.